transmission and coding of information

problem list

José Luis Ruiz
july 2018

Departament de Matemàtiques
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

Contents

1

Information and entropy

1.1 We toss a perfect coin and if we get tails it's over; if we get heads we toss it again and it's over. Find the entropy of the random variable associated to the result of the last toss.

1.2 We toss a coin and a dice, both perfect. Do we get more information in that experiment or in the one consisting of tossing three perfect coins? What happens if we toss four perfect coins?

1.3 How much information do we obtain when we draw a card from a deck of 52 cards in the following cases:

1) each card has the same probability of being drawn;

2) the probability of drawing a black card is twice the probability of drawing a red one.

1.4 We throw a perfect dice with two faces numbered with a 1, two faces numbered with a 2 and the other two faces numbered with a 3. Then we toss a perfect coin as many times as the dice indicates. Calculate the entropy of the random variable associated to this experiment.

1.5 The weather in two cities A and B can be in one of these four states: rainy, sunny, cloudy and foggy. In the city A the probabilities are $1/4$ for each state, and in the city B the probabilities are: $1/4$ for sunny, $1/8$ for rainy, $1/8$ for cloudy and $1/2$ for foggy. In which city do we need more information to know the weather?

1.6 [+] A random variable X has a binomial distribution:

$$p_k = p(X = k) = \binom{n}{k} p^k q^{n-k}, \qquad 0 < p < 1, \quad q = 1 - p.$$

Prove that $H(X) \leq -n(p \log p + q \log q)$.

1.7 [+] Prove that any swap of two probabilities in a finite distribution $p_1, \ldots, p_n$ that tends to approach to an equiprobable distribution increases the entropy. Concretely, if $p_1 > p_2$ and $0 \leq d < (p_1 - p_2)/2$, then $H(p_1, p_2, \ldots, p_n) \leq H(p_1 - d, p_2 + d, p_3, \ldots, p_n)$. [Hint: apply Gibbs' Lemma.]

1.8 Let $P = (p_1, \ldots, p_n)$, $Q = (q_1, \ldots, q_m)$ and $R = (\lambda, \mu)$ be finite probability distributions and define $S = \{\lambda p_1, \ldots, \lambda p_n, \mu q_1, \ldots, \mu q_m\}$.

1) Prove that S is also a finite probability distribution.

2) Compute the entropy of S.

3) Find the values of λ and μ that maximize this entropy.

1.9 Assume that X and Y are finite random variables taking the values 0 and 1. We know that $p(X = 0) = 1/3$, $p(Y = 0 \mid X = 0) = 1/4$, and $p(Y = 1 \mid X = 1) = 3/5$. Compute $H(X, Y)$, $H(X \mid Y)$, $H(Y \mid X)$, $H(Y)$ and $I(X, Y)$.

1.10 Let $p_1, \ldots, p_n$ be a finite probability distribution. Let $q_1, \ldots, q_m$ be the distribution defined by grouping some probabilities as follows:

$$q_1 = p_1 + \cdots + p_{i_1}, \quad q_2 = p_{i_1+1} + \cdots + p_{i_2}, \quad \text{etc}$$

Show that $H(q_1, \ldots, q_m) < H(p_1, \ldots, p_n)$. *Hint*: show that if $x, y > 0$, then:

$$(x + y) \log \frac{1}{x + y} < x \log \frac{1}{x} + y \log \frac{1}{y}.$$

1.11 We toss two perfect dice. Let X and Y be the random variables that give the value of each dice. Prove that $H(X + Y) < H(X) + H(Y)$. *Hint*: apply problem 1.10.

1.12 Let X and Y be finite random variables. Prove that $H(X + Y \mid X) = H(Y)$.

1.13 Prove that for every random variable X one has $H(X, X^2) = H(X)$. This means that $H(X^2 \mid X) = 0$. Check that $H(X \mid X^2)$ is not always 0.

1.14 Let (Ω, p) be a finite probability space and $X \colon \Omega \to \mathbb{R}$ a random variable. Let $f \colon \mathbb{R} \to \mathbb{R}$ be a function. We write "$f(X)$" to denote the composition $f \circ X$.

1) Show that $H(f(X) \mid X) = 0$.

2) Show that if f is a one-to-one function, then $H(X \mid f(X)) = 0$.

1.15 The random variable X takes the values $1, 2, \ldots, 2n$ with equal probability. Define the random variable Y as $Y = 0$, if X is even and as $Y = 1$ if X is odd. Prove that $H(X \mid Y) = H(X) - 1$, but $H(Y \mid X) = 0$.

1.16 A city has two neighborhoods A and B. We know that in an opinion poll, half the people from A always say the truth, 3/10 of them always lie and 2/10 never answer the poll. As for people from B, 3/10 of them always say the truth, the half always lie and 2/10 of them never answer the poll. Let p be the percentage of citizens from A and $I(p)$ the mutual information of the variables *belonging to one the neighborhoods* and *belonging to a group of answers*. Find the maximum value of $I(p)$ and the corresponding value of p.

1.17 The precision of a meteorologist from a radio station when predicting the weather is represented in the following table:

	It rains	It doesn't rain
Predicts it will rain	1/12	1/6
Predicts it won't rain	1/12	2/3

For example, one out of twelve times the weatherman predicts it will rain and it actually rains. As we can see the meteorologist gets it right 3 out of 4 times.

A man who is listening to the radio realizes that saying always it will not rain he can predict the weather correctly 5 out of 6 times. So the man goes to the radio station and asks for the meteorologist's job. However, the station manager refuses his petition. Why?

2

Codes

2.1 We want to build a prefix binary code that contains the words 0, 10 and 110. How many additional words of length 5 can this code have?

2.2 Can we deduce from Kraft's inequality that the following sets are binary codes?

1) $\mathcal{C} = \{001\,, 1001\,, 0010\,, 1110\,, 1010\,, 01110\,, 0101\}$.

2) $\mathcal{D} = \{00\,, 10\,, 011\,, 101\,, 111\,, 110\,, 010\}$.

2.3 Can we deduce from Kraft's inequality that the following sets are codes over their respective alphabets?

1) $\mathcal{C} = \{00\,, 01\,, 001\,, 100\,, 111\}$, $A = \{0, 1\}$.

2) $\mathcal{D} = \{00\,, 01\,, 02\,, 10\,, 11\,, 20\,, 0ab\,, 0000\,, 1111\,, 2222\}$, $A = \{0, 1, 2\}$, where moreover $a, b \in A$ take every possible value.

2.4 How many symbols are needed to construct a prefix code with four words of length 1 and twelve words of length 2?

2.5 Find the minimum length of a block code that encodes an alphabet with 26 letters $A, \ldots, Z$ with an alphabet with 3 symbols.

2.6 Determine in each case whether there exists a q-ary prefix code with the given lengths, and construct one when it exists.

1) $q = 2$, lengths: $1, 2, 2, 3, 3$;

2) $q = 2$, lengths: $1, 3, 3, 3, 4, 4$;

3) $q = 2$, lengths: $2, 2, 3, 3, 4, 4, 5, 5$;

4) $q = 3$, lengths: $1, 1, 2, 2, 3, 3, 3$;

5) $q = 3$, lengths: $1, 2, 2, 2, 2, 2, 3, 3, 3, 3$;

6) $q = 5$, lengths: $1, 1, 1, 1, 1, 8, 9$;

2.7 Let A be a finite alphabet. Let $\mathcal{C}$ be a prefix code over A for which Kraft's inequality is strict. Prove that it is possible to add a new word to $\mathcal{C}$ and extend it to another instantaneous code over the same alphabet. Do this construction explicit for an instantaneous binary code with the following lengths:

$$2\,, 3\,, 3\,, 4\,, 4\,, 4\,, 4\,, 7\,, 7\,, 7\,, 7\,, 7\,, 7.$$

3

Source coding

3.1 A discrete memoryless information source has the distribution:

$1/2, 1/4, 1/8, 1/16, 1/32, 1/32$

Find a binary and a ternary Huffman encodings for the source.

3.2 Construct a Huffman code over the alphabet $A = \{0, 1, 2\}$ from the given symbols and probabilities:

x_1	0.3	x_2	0.2	x_3	0.15	x_4	0.1
x_5	0.1	x_6	0.08	x_7	0.05	x_8	0.02

3.3 Consider the discrete memoryless information source $S = (A, X)$, where $A = \{0, 1, ?\}$ and $p(0) = 0.7$, $p(1) = 0.2$, $p(?) = 0.1$. Find Huffman binary encoding for S and for S^2. Compare the number of bits we use for S in both encodings with the entropy of the source.

3.4 We have a set of eight symbols with probabilities 0.2, 0.15, 0.15, 0.1, 0.1, 0.1, 0.1, 0.1. Construct a ternary Huffman code and check that the code $\{00, 01, 02, 10, 11, 12, 20, 21\}$ has also minimum average length.

3.5 A memoryless source emits the symbols a, b, c, d with probabilities 0.4, 0.3, 0.2 i 0.1, respectively. Find a binary encoding that does not require more that 1.87 bits per symbol.

3.6 Consider a memoryless source with the alphabet $A = \{a_1, \ldots, a_9\}$ with probabilities 1/4, 1/4, 1/8, 1/8, 1/16, 1/16, 1/16, 1/32 and 1/32. Can we encode it with an efficiency of 100%? If the answer is affirmative, which should be the length of the blocks to encode?

3.7 Write a binary encoding for the alphabet $A = \{a_1, \ldots, a_9\}$ so that there are two code-words with length 2 and three code-words with length 3. Write, if possible, a probability distribution for this memoryless source so that the above given encoding has an average length equal to the entropy. Write another distribution so that the average length of the encoding doesn't coincide with the entropy.

3.8 Let $S = (A, X)$ be a discrete memoryless information source with three symbols and probability distribution 0.5, 0.25, 0.25.

1) Find a binary Huffman encoding for the second extension of S.

2) Compute the minimum average length of the binary encondings of S^2.

3) Check the first Shannon theorem for S^2.

3.9 [+] Prove that in a binary Huffman code for a source with cardinal $n \geq 2$ and without null probabilities, the following equality is fulfilled:

$$\sum_{i=1}^{n} \frac{1}{2^{\ell_i}} = 1.$$

Is it true the above formula for a ternary Huffman code? *Hint*: proceed by simple induction on n in the binary case.

4

Channel coding

4.1 Consider the communication channel $K = (A, B, Q)$, where $A = \{0, 1\}$, $B = \{0, ?, 1\}$ and the matrix Q has the entries:

$$p(0 \mid 0) = 3/4, \quad p(? \mid 0) = 1/4, \quad p(? \mid 1) = p(1 \mid 1) = 1/2$$

Assume that we put the distribution X, given by $p(0) = 2/3$, $p(1) = 1/3$, at the input. Calculate the distribution $Y = K(X)$ that we get at the output and compute the mutual information $I(X, Y)$.

4.2 Find the mutual information of the channel given by the matrix:

$$\begin{bmatrix} 1/2 & 0 & 1/2 \\ 0 & 1/4 & 3/4 \\ 1/3 & 2/3 & 0 \end{bmatrix}$$

if we assume that the input symbols are equally likely.

4.3 Find the capacity of the following channel and the probability distribution at which it is attained.

$$\begin{bmatrix} 1/2 & 1/3 & 1/6 \\ 1/6 & 1/2 & 1/3 \\ 1/3 & 1/6 & 1/2 \end{bmatrix}.$$

4.4 Consider the channel $K = (A, B, Q)$, where:

$$Q = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & 0 & 1/2 \end{bmatrix}$$

1) Compute the output distribution $Y = K(X)$ if we consider the distribution $X = (p, 1 - p)$ at the input.

2) Compute the mutual information $I(X, Y)$, when $p = 1/4$.

3) Is there any input distribution giving an equally likely output distribution?

4.5 A channel is given by the matrix:

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Find its capacity and the input distribution that fulfills it.

4.6 A channel has as inputs the binary words of length 2 and as output the AND of the corresponding bits (that is, the channel behaves as an AND logic gate).

1) Write the channel's matrix, taking into account that the input alphabet has four symbols and the output alphabet has two symbols.

2) Assume that the probabilities of a 0 or a 1 in the input are p and q respectively. Calculate the information transmitted by the channel.

3) Study the capacity of this channel.

4.7 We say that a channel is *lossless* if every column in its matrix has at most one non-zero element. If X, Y are the input and the output random variables of the channel, prove that $H(X|Y) = 0$ and calculate the capacity of the channel.

4.8 Let $K_1 = (A, B, Q)$ and $K_2 = (B, C, R)$ be communication channels. We define a new channel $K_3 = (A, C, S)$ by connecting the output of K_1 with the input of K_2.

1) Show that $S = QR$.

2) Assume that both K_1 and K_2 are binary symmetric channels with error probabilities p_1 and p_2, respectively. Show that the corresponding K_3 is also a binary symmetric channel and calculate its capacity.

4.9 Let K_1 be the channel corresponding to a XOR gate (that is, K_1 has inputs 00, 01, 10, 11 and a binary output computed using a XOR). Let K_2 be a binary symmetric channel with error probability $p < 1/2$.

1) Show that K_1 is a deterministic channel and find its capacity.

2) Let K_3 be the channel we get by connecting the output of K_1 with the input of K_2. Find its matrix and show that there is an input distribution giving an equally likely output distribution. What can you say about the capacity of K_3?

5

Block codes

Note: In this chapter *code* refers to a block code.

5.1 Let x, y be two binary words of the same length. Prove the formula:

$$d(x,y) = |x| + |y| - 2|x \wedge y|,$$

where $x \wedge y$ denotes a bitwise AND.

5.2 Let $\mathcal{C}$ be a $(n, M, d)_q$-code and consider the code $\mathcal{C}'$ obtained from $\mathcal{C}$ by erasing the last $d-1$ last positions from all the codewords. Show that $|\mathcal{C}'| = M$.

5.3 Let $\mathcal{C}$ be a binary code of length n and odd minimum distance d. Show that the code $\overline{\mathcal{C}}$ obtained from $\mathcal{C}$ by adding an overall parity bit has minimum distance $d+1$.

$$\overline{\mathcal{C}} = \{x_1 \cdots x_n x_{n+1} \,:\, x_1 \cdots x_n \in \mathcal{C},\ \textstyle\sum_{i=1}^{n+1} x_i = 0\}$$

5.4 *The Singleton bound*. Prove that $A_q(n,d) \leq q^{n-d+1}$. (*Hint*: given a q-ary code $\mathcal{C}$ of type (n, M, d), consider the code $\mathcal{C}'$ obtained by erasing the last $d-1$ positions of every word in $\mathcal{C}$.)

5.5 Prove that $A_2(3,2) = 4$ and $A_3(3,2) = 9$. Generalize these results to $A_p(3,2)$, where p is a prime number. (*Hint*: use arithmetic modulo p.)

5.6 [+] Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be binary codes of types (n, M_1, d_1) and (n, M_2, d_2), respectively. Let $\mathcal{C}$ be the binary code of length $2n$ obtained by concatenating each word $x \in \mathcal{C}_1$ with every word $x + y$ for $y \in \mathcal{C}_2$. Prove that $\mathcal{C}$ is a binary code of type$(2n, M_1 M_2, d)$ where $d = \min(2d_1, d_2)$. We denote this code as $\mathcal{C}_1|\mathcal{C}_1 + \mathcal{C}_2$.

5.7 We define recurrently the codes $\mathcal{R}_n$, $n \geq 0$, as follows:

$$\begin{aligned}
&\mathcal{R}_0 = \mathbb{Z}_2^2 && \text{(total code of length 2)}\\
&\mathcal{R}_1 = \mathcal{R}_0|\mathcal{R}_0 + \mathrm{Rep}(2)\\
&\mathcal{R}_n = \mathcal{R}_{n-1}|\mathcal{R}_{n-1} + \mathrm{Rep}(2^n), && \text{si } n \geq 2,
\end{aligned}$$

where $\mathrm{Rep}(m)$ is the binary repetition code of length m. Find the parameters of this family of codes. These are the Reed-Muller codes of the first kind.

6

Finite fields

6.1 Let $p_1(x) = x^3 + 1$ and $p_2(x) = x^4 + x^3 + x^2 + x + 1$ be polynomials over $\mathbb{F}_2$. Find $d(x) = \gcd(p_1(x), p_2(x))$ and polynomials $a(x), b(x) \in \mathbb{F}_2[x]$ satisfying the Bézout identity:

$$a(x)p_1(x) + b(x)p_2(x) = d(x).$$

6.2 Find all primitive elements in the fields $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$ and $\mathbb{F}_{13}$. Write every nonzero element as a power of a primitive element in each field, chosen previously.

6.3 Find all irreducible polynomials over $\mathbb{F}_2[x]$ up to degree 6. Which polynomials are primitive?

6.4 Let $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1)$ and let $\alpha = \overline{x}$. Compute the inverses of the elements $1 + \alpha$ and $1 + \alpha^2 + \alpha^3$ and write the invers of $1 + \alpha$ as a sum of powers of itself.

6.5 Calculate the inverses of the elements α, $1 + \alpha^2 + \alpha^3$ and $1 + \alpha^3 + \alpha^4$ in the field $\mathbb{F}_{64} = \mathbb{F}_2[x]/(1 + x + x^6)$, where $\alpha = \overline{x}$. Find a primitive element of this field.

6.6 Check that the polynomial $f(x) = x^3 + x^2 + 1$ is irreducible over $\mathbb{F}_2$. Let $\alpha = \overline{x}$ in the finite field $\mathbb{F}_8 = \mathbb{F}_2[x]/(f(x))$ of 8 elements.

1) Prove that α is a primitive element of $\mathbb{F}_8$.

2) Represent all the elements of $\mathbb{F}_8$ as powers of α.

3) Find the table of Zech's logarithms with respect to α.

4) Simplify the expression:

$$\frac{(\alpha^2 + \alpha^6 - \alpha + 1)(\alpha^3 + \alpha)}{\alpha^4 + \alpha}$$

6.7 Let $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$, $\mathbb{F}_8 = \mathbb{F}_2[x]/f(x)$ and $\alpha = \overline{x}$ (check that α is a primitive element). Solve the following linear systems in the unknowns u, v and w with coefficients in $\mathbb{F}_8$.

$$\left.\begin{aligned} u + v + w &= 1 + \alpha \\ (1+\alpha)u + (1+\alpha^2)v + \alpha^3 w &= 0 \\ (1+\alpha)u + \alpha^2 v + \alpha w &= 1 + \alpha + \alpha^2 \end{aligned}\right\} \qquad \left.\begin{aligned} (1+\alpha)u + (1+\alpha^2)v + \alpha^3 w &= 0 \\ (1+\alpha)u + \alpha^2 v + \alpha w &= 0 \end{aligned}\right\}$$

6.8 Consider the finite field $\mathbb{F}_{16}$ of cardinal 16 built from the polynomial $f(x) = x^4 + x^3 + 1$ over $\mathbb{F}_2$.

1) Check that this polynomial is irreducible over $\mathbb{F}_2$.

2) Prove that $\alpha = \overline{x} \in \mathbb{F}_{16}$ is a primitive element of this field.

3) Compute the orders of the elements α^4, $\alpha + \alpha^2$ and α^5.

6.9 Prove that the polynomial $f(x) = x^5 + x^2 + 1$ is irreducible and primitive over $\mathbb{F}_2$. Hence, it defines the finite field $\mathbb{F}_{32}$. Let α be the class of x in this field.

1) Write the element:

$$\beta = \alpha^5 + \alpha^{23} + \frac{\alpha^2 + \alpha^4}{1 + \alpha^{12}}$$

as a power of α.

2) Solve in $\mathbb{F}_{32}$ the quadratic equation $\alpha^3 t^2 + \alpha^{18} t + 1 = 0$.

6.10 Solve the equation $\alpha^3 x^3 + \alpha^2 x^2 + \alpha^6 x + 1 = 0$ in the field $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, where $\alpha = \overline{x}$.

6.11 Let $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$ and $\alpha = \overline{x}$. Consider the polynomial:

$$p(x) = x^{13} + x^{12} + x^6 + x^5 + x^4 + x^2 + x + 1.$$

Compute the values $p(\alpha^i)$, for $i = 1, \ldots, 6$.

6.12 Consider $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$ and let $\alpha \in \mathbb{F}_{16}$ be the class of x. Find the greatest common divisor of the polynomials with coefficients in $\mathbb{F}_{16}$:

$$a(t) = t^4, \quad b(t) = \alpha^{11} t^3 + \alpha^5 t^2 + \alpha^{13} t + \alpha^{14},$$

and write the corresponding Bézout identity.

6.13 Let $p(x) \in \mathbb{F}_2[x]$ be a polynomial with binary coefficients and let α be an element of some finite field $\mathbb{F}_{2^m}$ containing $\mathbb{F}_2$. Prove that if $p(\alpha) = 0$, then $p(\alpha^2) = 0$.

7

Linear Codes

Note: all codes in this section are binary, unless the contrary is stated explicitly.

7.1 A linear code of length 8 is defined by the following equations:

$$\begin{aligned} x_5 &= x_2 + x_3 + x_4 \\ x_6 &= x_1 + x_2 + x_3 \\ x_7 &= x_1 + x_2 + x_4 \\ x_8 &= x_1 + x_3 + x_4 \end{aligned}$$

Find a parity-check matrix, show that the minimum distance is 4 and determine the number of words of weight i, $(0 \leq i \leq 8)$.

7.2 Find all words, the minimum distance and a parity-check matrix for the binary linear code of type $[5, 3]$ defined by the generator matrix:

$$G = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

7.3 Find a generator matrix of the linear code that has the following matrix as a parity-check matrix:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

7.4 Find parity-check matrices for the linear codes defined over the finite field $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$ and given by the following generator matrices:

$$\begin{pmatrix} 1 & \alpha & 0 & 0 & 1+\alpha & 0 \\ 0 & 0 & \alpha & 1 & 0 & \alpha \\ 0 & 1 & 0 & \alpha & 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \end{pmatrix},$$

where α is the class of x. Compute the parameters of these codes.

7.5 Consider the linear code $\mathcal{C}$ defined over the finite field $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$ given by the following parity-check matrix:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Compute a generator matrix for $\mathcal{C}$ and its parameters.

7.6 How does the parity-check matrix of a code change when we extend this code by a parity-check bit?

7.7 Prove that in a linear code either all the codewords have an even number of ones or half the codewords have an even number of ones and the other half an odd number of ones.

7.8 Let $n = rs$. Let $\mathcal{C}$ be the binary code of length n composed by the words $x = a_1 a_2 \dots a_n$ such that, when written in table form

$$\begin{array}{ccc} a_1 & \cdots & a_r \\ a_{r+1} & \cdots & a_{2r} \\ \vdots & & \vdots \\ a_{(s-1)r+1} & \cdots & a_{sr}, \end{array}$$

the sum of every row and every column is zero.

1) Check that $\mathcal{C}$ is a linear code. What is its dimension? What is its minimum distance?

2) Think of a decoding strategy.

3) If this is the 2-dimensional case, what is the 3-dimensional case like?

4) Compute a generator matrix and a parity-check matrix for the case $r = 3$ and $s = 4$.

7.9 Describe the way of decoding the binary repetition code of length 7 in order to correct 2 errors and to detect 4 at the same time. If we only want to correct one error, how many of them can we detect then?

7.10 Calculate the syndromes and leaders of the binary repetition code of length 7.

7.11 Calculate the syndromes and leaders of the code defined over the finite field $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$ given by the following generator matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha \\ 0 & 0 & 1 & 1 & 1+\alpha \end{pmatrix},$$

where α is the class of x.

7.12 A binary linear code $\mathcal{C}$ is given by the following parity-check matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Find the cosets of $\mathcal{C}$, the leaders and the syndromes. If we receive the word $y = 01001$, what is the most likely message sent?

7.13 Consider the alphabet:

$$A = \{space, e, h, l, m, p, u, a\}.$$

We want to send messages over A through a binary symmetric channel. To do that, we assign to each symbol of A a binary word of length 4 as indicated in the following table:

$$\begin{array}{llllll} space & \mapsto 0011 & m & \mapsto 0010 & e & \mapsto 1100 \\ p & \mapsto 1101 & h & \mapsto 0110 & u & \mapsto 1010 \\ l & \mapsto 0100 & a & \mapsto 0101. & & \end{array}$$

Afterwards we encode these words of length 4 with the linear code with generator matrix:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

At the other end of the channel we get the following binary message:

$$11010110 \quad 10001011 \quad 10011000 \quad 10101101 \quad 11110100 \quad 01000110 \quad 10100101.$$

Decode this message and find the most likely message over A that was sent.

7.14 Consider the code described by the check matrix:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

1) Write down the parameters of the code.

2) Give a systematic generator matrix (if it exists; otherwise, give a non-systematic one).

3) Encode the message composed uniquely of ones with the above generator matrix.

4) Find the minimum distance of this code.

5) Build a decoding table for correcting error patterns up to one error.

6) Using the above table, estimate the errors introduced by the channel in the words 011001, 111110, 111111.

7.15 Find a generator matrix and a parity-check matrix of a ternary Hamming code of length 4.

7.16 Encode the message:

1010 0010 1110 1001 0110 0101 0111 0010
0101 1110 1011 1000 0000 0011 0101 1011

with a Hamming code of length 7.

7.17 Find a check matrix of a Hamming code over $\mathbb{F}_7$ of length 8. Use this matrix to decode the message 3523410610521360.

7.18 Find a check matrix of a Hamming code over $\mathbb{F}_4$ of codimension 2 and decode the message $0\alpha\alpha11$, where $\alpha \in \mathbb{F}_4$ is a primitive element.

7.19 The extended binary Hamming code $\mathrm{Ham}'(r,2)$ is the code obtained from $\mathrm{Ham}(r,2)$ adding a parity bit to all codewords.

1) Determine the parameters of $\mathrm{Ham}'(r,2)$.

2) Find a parity-check matrix of $\mathrm{Ham}'(3,2)$.

3) Find an explicit algorithm for correcting one error and detecting two at the same time with $\mathrm{Ham}'(3,2)$.

7.20 [*Singleton bound for linear codes.*] Prove that any linear code of type $[n,k,d]_q$ fulfills the inequality $k+d \leq n+1$.

7.21 Detect and/or correct the errors in the following ISBN codewords:

1) 84-7223-954-3;

2) 84-7635-458-X;

3) 0-38?-94599-7;

4) 0-7923-4688-8, if we know that there one error of size 2.

7.22 Detect and/or correct the errors in the following DNI numbers:

1) 42.726.135-N;

2) 36.401.301-Y;

3) 46.00?.002-J;

4) 49.761.170-T, if we know that there is one error of size 4.

7.23 The EAN (*European Article Number*) code consists of the words of length 13 over $\mathbb{Z}_{10}$ such that:

$$u \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1)^T = 0,$$

where the operations are done in $\mathbb{Z}_{10}$.

1) Show that this code detects simple error patterns.

2) Determine which errors consisting in the transposition of two adjacent digits this code can detect.

[*Note*: the first two digits of u determine the country; the following five represent the manufacturer; the following five the product; and the last digit is a check digit computed by solving for it in the above formula. The EAN code is usually represented by means of a bar-code.]

7.24 The identity number of the passports in some countries is a word of length 7 over $\mathbb{Z}_{10}$. The first six digits represent the birth date in the form:

x_1x_2	x_3x_4	x_5x_6
day	month	year

The last digit x_7 is computed from the equation:

$$x_7 + 7(x_1 + x_4) + 3(x_2 + x_5) + x_3 + x_6 = 0$$

in $\mathbb{Z}_{10}$. Show that this code can detect simple error patterns and study its behavior with respect to a transposition of adjacent digits.

7.25 Since the year 1966, Norway's citizens have been assigned an identification number $x_1x_3x_3\cdots x_{11}$ of 11 decimal digits. The first six digits represent the birth date, $x_7x_8x_9$ is a personal number and $x_{10}x_{11}$ are check digits defined by the system of equations:

$$x_{10} = -(3x_1 + 7x_2 + 6x_3 + x_4 + 8x_5 + 9x_6 + 4x_7 + 5x_8 + 2x_9)$$
$$x_{11} = -(5x_1 + 4x_2 + 3x_3 + 2x_4 + 7x_5 + 6x_6 + 5x_7 + 4x_8 + 3x_9 + 2x_{10})$$

where the operations are done in the finite field $\mathbb{F}_{11}$. Consider the linear code defined by these equations over $\mathbb{F}_{11}$. Determine a parity-check matrix. If we use this code for detecting errors, which double error patterns cannot we detect?

7.26 The *Zip* postal code in the USA is a code whose words are of length 10 over $\mathbb{Z}_{10}$. The first digit represent one of the 10 geographical zones (from 0 corresponding to the northeast to 9 that corresponds to the west); the following two digits correspond to a post delivery center; the following two identify either a town or a local post office. Up to 1963 this code had six digits, but four more digits were added on 1983 to make the ordering tasks easier. The first two new digits determine a delivery sector and the other digits specify an area, for example one floor in a skyscraper. The tenth digit is a check digit defined by:

$$\sum_{i=1}^{10} a_i = 0$$

with the operations done in $\mathbb{Z}_{10}$. In order to facilitate the machine-reading process each digit is represented by means of a sequence of three short and two long bars according to the following scheme:

1	2	3	4	5	6	7	8	9	0
ıı|||	ıı|ı||	ıı||ı|	ıı|ı|ı|	ıı||ı|ı	ıı|ı|ı|ı	ıı||ı|ı	ıı|ı|ı|ı	ıı||ı|ı	ıı|ı|ı|ı

Moreover, there are two long bars, one at the beginning and one at the end of the word.

1) The *Zip* code of North Carolina State University is 27695-8205x. Determine the last check digit.

2) Determine the *Zip* code represented by the bar-code:

3) Show that a single error made by the bar-code reader can be detected.

4) Show that we can correct one error if we know its the position.

5) Use the last result to correct the codeword:

6) Show we can detect two errors in a block of five bars, but not always correct them.

8

Cyclic codes

8.1 Factor the polynomials $x^n - 1$ in $\mathbb{F}_2[x]$, for $n = 3, 5, 7, 9, 11, 13$.

8.2 Find all binary cyclic codes of lengths 5, 7 and 9. Check that the binary cyclic code of length 7 with generator polynomial $1 + x^2 + x^3$ is equivalent to a Hamming code.

8.3 Let $\mathcal{C}$ be a binary cyclic code of length 23 and dimension k such that $1 < k < 22$. Show that $k = 11$ or $k = 12$.

8.4 Let $\mathcal{C}$ be a binary cyclic code of odd length. Prove that $\mathcal{C}$ has a codeword of odd weight if and only if $11 \cdots 1 \in \mathcal{C}$.

8.5 Check that the polynomial $1 + x + x^2 + x^3$ generates a binary cyclic code with parameters $[8, 5]_2$. Encode the message 10101 in a systematic way.

8.6 Encode systematically the message 1101 with a binary cyclic code of length 7 with generator polynomial $1 + x^2 + x^3$.

8.7 Write down all the codewords of the binary cyclic code of length 6 and generator polynomial $1 + x + x^3 + x^4$. Compute the minimum distance of this code.

8.8 What is the minimum possible length of a binary cyclic code with generator polynomial $x^4 + x^3 + x^2 + 1$? Find a parity-check matrix and compute the minimum distance. Write equations for a systematic encoding and make explicit the Meggitt algorithm in this case.

8.9 A binary cyclic code has generator polynomial $x^6 + x^2 + 1$ and the least possible length.

1) Find the number of information and check bits in a codeword.

2) Find the cardinal of the code.

3) Calculate a generator matrix and a parity-check matrix.

4) Find the minimum distance.

5) Explain how to encode systematically with this code and how to apply Meggitt algorithm.

8.10 Consider the binary cyclic code of length 15 with generator polynomial $1+x+x^4$. Encode systematically the message 11001101011. Decode the word 000010001101011 using the Meggitt algorithm.

8.11 Let $\mathcal{C}$ be the binary cyclic code $[15,7]_2$ with generator polynomial $g(x) = 1+x^4+x^6+x^7+x^8$. This code has minimum distance $d = 5$.

1) Encode the word 1101001 with a systematic encoding.

2) Apply the Meggitt algorithm to decode the received word 100010001101110

8.12 Let C be the cyclic code of length 9 and generator polynomial $g(x) = x^6+x^3+1$. We accept that the minimum distance is $d = 3$.

1) Encode systematically the message 011.

2) Apply the Meggitt algorithm to decode the received word 101101111.

8.13 Let C be the cyclic code of length 7 and generator polynomial $g(x) = x^4+x^3+x^2+1$. We accept that the minimum distance is $d = 3$.

1) Show that all the codewords have even weight.

2) Encode systematically the message 001101.

3) Apply the Meggitt algorithm to decode the message 0101111 1001111.

8.14 Decode the following words using the BCH code consisting of the polynomials $c(x)$ of degree ≤ 14 such that $c(\alpha) = c(\alpha^3) = 0$, where $\alpha \in \mathbb{F}_{16}$ is a primitive element (this code is the same as the one found in the slides).

1) 110001100011110;
2) 000000111010001;
3) 110110110001100;
4) 111011000111111;
5) 001000011010001;
6) 010010111110001.

9 BCH and Reed-Solomon codes

9.1 BCH codes

All BCH codes in this section are binary.

9.1 Consider the 3-error-correcting BCH code $\mathcal{C}$ of length 15. We use the finite field $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$.

1) Compute the generator polynomial $g(x)$.

2) Encode systematically the message composed by two 1's and thirteen 0's.

9.2 Compute the parameters of the BCH code of length 31 and designed minimum distance 7.

9.3 A binary BCH code $\mathcal{B}$ of length 15 has $\alpha^3, \alpha^4, \alpha^5$ among its roots, where α belongs to a suitable auxiliary finite field $\mathbb{F}_q$. Determine the dimension of $\mathcal{B}$ and a lower bound for its minimum distance.

9.4 Let $\mathcal{C}$ be the binary BCH code of length $n = 31$ and designed minimum distance $\delta = 7$ and auxiliary finite field $\mathbb{F}_{32} = \mathbb{F}_2[x]/(x^5 + x^2 + 1)$.

1) Find the generator polynomial $g(x)$ of $\mathcal{C}$.

2) Find the number of information bits and the number of parity-check bits in every codeword. How many errors can this code correct at least?

3) Encode systematically the message $M = 0111010111010001$.

4) We have received the word $y = 0\,00011\,11000\,01000\,01101\,01111\,00000$. Find the syndrome polynomial $s(x)$ of y.

5) Apply the algorithm based in the Euclides algorithm and the Bézout identity to correct the errors that y may have. *Hint*: the following computations may be useful:

$$\begin{aligned} x^6 &= s(x)(\alpha^{22}x + \alpha^{26}) + r_1(x), & \deg(r_1) &= 4 \\ s(x) &= r_1(x)(\alpha^{25}x + \alpha^8) + r_2(x), & \deg(r_2) &= 3 \\ r_1(x) &= r_2(x)(\alpha^6 x + \alpha^2) + r_3(x), & \deg(r_3) &= 2 \end{aligned}$$

where $\alpha \in \mathbb{F}_{32}$ is the class of x.

6) Repeat the last two questions for each one of the following words:

$$y_1 = 0000\,0000\,0000\,0000\,1000\,1011\,0001\,001$$
$$y_2 = 1000\,1000\,1000\,0000\,1000\,1011\,0001\,001$$
$$y_3 = 0000\,0001\,0001\,0001\,1000\,1011\,0001\,001$$

9.5 Let $\mathcal{C}$ be the binary BCH code of length $n = 15$ and designed distance $\delta = 5$ with auxiliary finite field $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$.

1) Check that the generating polynomial of $\mathcal{C}$ is $g(x) = x^8 + x^7 + x^6 + x^4 + 1$.

2) Find the dimension of the code and a lower bound for its minimum distance.

3) Encode systematically the message $M = 0111010$.

4) Apply the algorithm based on the quadratic equation to decode the word $y = 11001\,11000\,01111$. Start by computing the syndromes $y(\alpha)$ and $y(\alpha^2)$.

5) Apply the algorithm based on the Euclid's algorithm and the Bézout's identity to correct the errors in y. Start by computing the syndrome polynomial $s(x)$ and use the following computations:

$$\begin{aligned} x^4 &= s(x)(\alpha^{12}x + \alpha^5) + r_1(x), && \deg(r_1) = 2 \\ s(x) &= r_1(x)(\alpha^7 x) + r_2(x), && \deg(r_2) = 1 \end{aligned}$$

where $\alpha \in \mathbb{F}_{16}$ is the class of x.

6) Find the syndrome polynomial $s(x)$ of $z = 110\,0100\,0001\,1111$ and apply the algorithm based on the Euclid's algorithm to correct the errors in z, if any. The following information could be useful:

$$\begin{aligned} x^4 &= s(x)(\alpha^{11}x + \alpha^{12}) + r_1(x), && \deg r_1(x) = 2 \\ s(x) &= r_1(x)(\alpha^5 x + \alpha) + r_2(x), && \deg r_2(x) = 0. \end{aligned}$$

where now $s(x)$ is the syndrome polynomial of z. Apply also the error-correcting algorithm based on the quadratic equation and check that both results are the same.

7) Find the syndrome polynomial $s(x)$ of the $w = 110\,0101\,1100\,1110$ and apply the algorithm based on the Euclid's algorithm to correct the errors in the w, if any. The following information could be useful:

$$\begin{aligned} x^4 &= (\alpha x)s(x) + r_1(x), && \deg r_1(x) = 3 \\ s(x) &= \alpha^8 r_1(x) + r_2(x), && \deg r_2(x) = 2 \\ r_1(x) &= (\alpha^4 x + \alpha^{13})r_2(x) + r_3(x), && \deg r_3(x) = 1. \end{aligned}$$

9.6

1) Show that the polynomial $f(x) = x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$ is primitive. Let $\mathbb{F}_{64}$ be the finite field defined by $f(x)$ and let $\alpha = \overline{x} \in \mathbb{F}_{64}$.

2) Consider the binary, strict and primitive BCH code $\mathcal{B}$ of length 63 with designed distance $\delta = 10$. Find the cyclotomic classes involved in the computation of the generating polynomial $g(x)$ of $\mathcal{B}$.

3) Compute the generating polynomial $g(x)$ of $\mathcal{B}$.

4) Find the dimension of $\mathcal{B}$ and give a lower bound for the minimum distance d and for the number of errors that $\mathcal{B}$ can correct. Can these bounds be improved?

5) Encode systematically the word M composed of a sequence of 12 ones, followed by a sequence of 12 zeros, followed by another sequence of 12 ones. Let N be the result of the encoding.

6) We send the word N and the channel introduces 2 errors, at positions 18 and 40. Let N' be the word received. Apply the algorithm based on the quadratic equation to correct the errors in N' (of course, you have to get the above positions 18 and 40).

7) Apply the euclidean algorithm to correct the errors in the following word:

$$P = 011110\ 010001\ 000000\ 100001\ 101111$$
$$000111\ 000111\ 000011\ 001111\ 010111\ 100$$

9.2 Reed-Solomon codes

9.7 Consider the finite field $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$ and the primitive element $\alpha = \overline{x} \in \mathbb{F}_8$. Consider the word $w = (0, \alpha, \alpha^2, 1, 1, 0, \alpha^5) \in \mathbb{F}_8^7$.

1) Compute the finite Fourier transform of w with respect to α.

2) Compute the inverse finite Fourier transform of w with respect to α.

9.8 Consider the Reed-Solomon code $\mathcal{C} = \mathcal{R}(16, 7)$, where the finite field $\mathbb{F}_{16}$ is built up using the polynomial $x^4 + x + 1$.

1) Compute its parameters and its generating polynomial.

2) Correct the following words:

   a) $(0, \alpha^3, \alpha, \alpha^5, \alpha^3, \alpha^2, \alpha^6, \alpha^{10}, \alpha, 0, 0, 0, 0, 0, 0)$

   b) $(1, \alpha^4, \alpha^2, \alpha, 0, 0, 1, 0, \alpha, \alpha^5, \alpha^3, \alpha^2, 0, \alpha^{10}, \alpha)$

   c) $(\alpha, 0, \alpha^7, 0, \alpha^{12}, \alpha^3, \alpha^3, 1, 0, 0, 0, 0, 0, 0, 0)$

9.9 Consider the Reed-Solomon code $\mathcal{C} = \mathcal{R}(16, 5)$, where the finite field $\mathbb{F}_{16}$ is built up using the polynomial $x^4 + x + 1$.

1) Compute its parameters and its generating polynomial.

2) Correct the following words:

a) $(0, 0, 1, \alpha^8, 0, 0, \alpha^5, 0, 0, 0, 0, 0, 0, 0, 0)$

b) $(0, \alpha^{10}, 0, \alpha^6, \alpha^{13}, 0, \alpha^8, \alpha^{11}, \alpha^3, \alpha^5, 0, 0, 0, 0, 0)$

c) $(\alpha^4, 0, 1, 0, 0, \alpha^2, \alpha^5, \alpha^{12}, \alpha^{14}, 0, 0, 0, 0, 0, 0)$

9.10 Consider the Reed-Solomon code $\mathcal{C} = \mathcal{R}(16, 9)$, where the finite field $\mathbb{F}_{16}$ is built up using the polynomial $x^4 + x + 1$. We have sent a word encoded with $\mathcal{C}$. Determine the most likely error occurred during the transmission if the received word has the following syndromes. (We write $s = (s_0, s_1, \ldots, s_7)$.)

1) $s = (\alpha^2, \alpha^8, \alpha^4, \alpha^5, \alpha^5, \alpha^7, \alpha^8, \alpha^9)$;

2) $s = (\alpha^2, 0, 0, \alpha^2, 0, \alpha, \alpha^{12}, 1)$;

3) $s = (\alpha^9, \alpha^{13}, \alpha^7, \alpha^4, \alpha^{12}, \alpha^4, \alpha^8, \alpha^2)$.

10

Solutions

10.1 Information and entropy

1.1 The probability of heads and tails is 1/4 and 3/4, respectively. Hence, the entropy of the associated random variable X is:

$$H(X) = -\frac{1}{4}\left(\log\frac{1}{4} + 3\log\frac{3}{4}\right) = 0.811278.$$

1.2 All three distributions are equally likely of respective probabilities 1/12, 1/8 and 1/16, and therefore the amount of information contained in them is $\log 12 = 3.58$, $\log 8 = 3$ and $\log 16 = 4$, respectively.

1.3 In the first case, the entropy is $\log 52$ because it corresponds to an equally likely distribution. In the second case, the probability that we draw a black card from the deck is $p_B = 1/39$ and the probability that we draw a red one is $p_R = 1/78$. Hence, the information in each case is:

$$\begin{aligned} I(\textit{red card}) &= \log 78 = 6.2854 \\ I(\textit{black card}) &= \log 39 = 5.2854 \end{aligned}$$

and the entropy is:

$$H = \frac{26}{78}\log 78 + \frac{26}{39}\log 39 = 5.6187.$$

1.4 The associated random variable has the following distribution:

$$\frac{1}{6}, \frac{1}{6}, \frac{1}{12}, \frac{1}{12}, \frac{1}{12}, \frac{1}{12}, \frac{1}{24}, \frac{1}{24}, \frac{1}{24}, \frac{1}{24}, \frac{1}{24}, \frac{1}{24}, \frac{1}{24}, \frac{1}{24},$$

and, therefore, the entropy is 3.58496.

1.5 More information is needed in the city A, because the maximum entropy is attained at an equally likely distribution.

1.6 We give two solutions to this problem. The first solution takes into account that a binomial distribution is the sum of n independent Bernouilli distribution with the same parameters. The second solution is a direct computation.

Solution 1. The variable X is the sum of n independents Bernoulli variables $X_1, \ldots, X_n$ with the same parameters. The entropy of a Bernoulli variable is:

$$H(X_i) = -(p \log p + q \log q);$$

hence:

$$H(X) = H(X_1 + \cdots + X_n) \leq H(X_1) + \cdots + H(X_n) = -n(p \log p + q \log q).$$

We have used the following property: if X and Y are random variables, then $H(X + Y) \leq H(X, Y)$. In effect, we have:

$$p(X + Y = c) = \sum_{a+b=c} p(X = a, Y = b)$$

so it is enough to show that if $0 \leq p, q \leq 1$, then $(p + q) \log \frac{1}{p+q} \leq p \log \frac{1}{p} + q \log \frac{1}{q}$. And that is easy to verify.

Solution 2.

$$\begin{aligned}
H(X) &= -\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \log \binom{n}{k} p^k q^{n-k} \\
&= -\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \log \binom{n}{k} \\
&\quad -\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} k \log p \\
&\quad -\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} (n-k) \log q \\
&= -\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \log \binom{n}{k} - n(p \log p + q \log q) \\
&\leq -n(p \log p + q \log q)
\end{aligned}$$

where we have applied the following properties:

$$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} k = pn, \qquad \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \log \binom{n}{k} \geq 0.$$

(The first equality gives the expectation value of a binomial distribution.)

1.7 Write $A = \sum_{i\geq 3} p_i \log(1/p_i)$. We have:

$$\begin{aligned} H(p_1', p_2', \ldots, p_n') &= p_1' \log \frac{1}{p_1'} + p_2' \log \frac{1}{p_2'} + A \\ &= (p_1 - d) \log \frac{1}{p_1 - d} + (p_2 + d) \log \frac{1}{p_2 + d} + A \\ &= p_1 \log \frac{1}{p_1 - d} + p_2 \log \frac{1}{p_1 - d} + A + d \log \frac{p_1 - d}{p_2 + d} \\ &\geq p_1 \log \frac{1}{p_1 - d} + p_2 \log \frac{1}{p_2 + d} + A \\ &\geq H(p_1, p_2, \ldots, p_n), \end{aligned}$$

the first inequality follows from $d \log\left((p_1 - d)/(p_2 + d)\right) \geq 0$ and the second one from Gibbs' lemma.

1.8

1) We have:

$$\begin{aligned} H(Z) &= -\sum_{i=1}^{n} \lambda p_i \log(\lambda p_i) - \sum_{j=1}^{m} \mu q_j \log(\mu q_j) \\ &= -\lambda \sum_{i=1}^{n} (p_i \log \lambda + p_i \log p_i) - \mu \sum_{j=1}^{m} (q_j \log \mu + q_j \log q_j) \\ &= -\lambda \log \lambda + \lambda H(X) - \mu \log \mu + \mu H(Y). \end{aligned}$$

2) The maximum value of the above function is attained at $\lambda = e^B/(1 + B)$, where $B = \exp(H(Y) - H(X))/\log 2$.

1.9

a) Distribution of X: $p(X = 0) = 1/3$, $p(X = 1) = 2/3$.

b) Distribution of $Y|X = 0$: $p(Y = 0|X = 0) = 1/4$, $p(Y = 1|X = 0) = 3/4$.

c) Distribution of $Y|X = 1$: $p(Y = 0|X = 1) = 2/5$, $p(Y = 1|X = 1) = 3/5$.

d) Distribution and entropy of Y:

$$\begin{aligned} p(Y = 0) &= p(X = 0)p(Y = 0|X = 0) + p(X = 1)p(Y = 0|X = 1) \\ &= \frac{1}{3} \cdot \frac{1}{4} + \frac{2}{3} \cdot \frac{2}{5} = \frac{7}{20} \\ p(Y = 1) &= 1 - p(Y = 0) = \frac{13}{20} \\ H(Y) &= H\left(\frac{7}{20}, \frac{13}{20}\right) = 0.94 \,\text{bits} \end{aligned}$$

e) Joint distribution and joint entropy of X and Y:

$$p(X=0,Y=0) = p(X=0)p(Y=0|X=0) = \frac{1}{3}\cdot\frac{1}{4} = \frac{1}{12}$$
$$p(X=0,Y=1) = p(X=0)p(Y=1|X=0) = \frac{1}{3}\cdot\frac{3}{4} = \frac{1}{4}$$
$$p(X=1,Y=0) = p(X=1)p(Y=0|X=1) = \frac{2}{3}\cdot\frac{2}{5} = \frac{4}{15}$$
$$p(X=1,Y=1) = p(X=1)p(Y=1|X=1) = \frac{2}{3}\cdot\frac{3}{5} = \frac{6}{15}$$
$$H(X,Y) = H\left(\frac{1}{12},\frac{1}{4},\frac{4}{15},\frac{6}{15}\right) = 1.84\,\text{bits}$$

f) Conditioned entropy $H(X|Y)$:

$$H(X|Y) = H(X,Y) - H(Y) = 1.84 - 0.94 = 0.9\,\text{bits}$$

g) Mutual information $I(X,Y)$:

$$I(X,Y) = H(X) - H(Y|X) = 0.92 - 0.9 = 0.02\,\text{bits}$$

1.11 We have $H(X) = H(Y) = \log 6$ and $H(X,Y) = H(X\times Y) = H(X) + H(Y)$, because they are independent variables. The distribution of $X+Y$ is obtained by grouping some of the probabilities of $X\times Y$, and in this process the entropy decreases (see problem 1.10). Concretely:

$$H(X+Y) = H\big(\frac{1}{36},\frac{2}{36},\ldots,\frac{1}{36}\big) < H\big(\frac{1}{36},\ldots,\frac{1}{36}\big) = H(X,Y) = H(X) + H(Y).$$

1.13 We distinguish two cases in the expression for the conditioned entropy:

$$H(X^2 \mid X) = \sum_{i,j} p(X^2 = y_j, X = x_i)\log\frac{1}{p(X^2 = y_j \mid X = x_i)}$$

Case 1. If $y_j = x_i^2$, then $p(X^2 = y_j \mid X = x_i) = 1$ and the corresponding summand is zero.

Case 2. If $y_j \neq x_i^2$, then $p(X^2 = y_j \mid X = x_i) = 0$ and the corresponding summand is also zero ($0\cdot\log(1/0) = 0$).

Hence, $H(X^2 \mid X) = 0$ and $H(X, X^2) = H(X)$.

On the other hand, let's consider the variable X that takes the values $0, 1, -1$ with the same probability. Then X^2 takes the values $0, 1$ with probabilities $1/3$ and $2/3$, respectively. Therefore:

$$H(X) = \log 3 \quad\text{and}\quad H(X^2) = (\log 3 + 2\log(3/2))/3 \neq \log 3;$$

that is, $H(X \mid X^2) \neq 0$.

1.15 It results from the definition of Y that its distribution is equally likely with probabilities 1/2 and 1/2. Hence, $H(Y) = 1$. The variable X is also an equally likely distribution and $H(X) = \log(2n)$. The conditioned entropy $H(X \mid Y)$ is given by the formula:

$$\begin{aligned} H(X \mid Y) &= p(Y=0)H(X \mid Y=0) + p(Y=1)H(X \mid Y=1) \\ &= \frac{1}{2}\left(H(X \mid Y=0) + H(X \mid Y=1)\right). \end{aligned}$$

Let's compute, for example, the term $H(X \mid Y=0)$; the other one is done analogously.

$$\begin{aligned} H(X \mid Y=0) &= \sum_{i=1}^{2n} p(X=i \mid Y=0) \log \frac{1}{p(X=i \mid Y=0)} \\ &= \sum_{\substack{i=0 \\ i \text{ even}}}^{2n} \frac{1}{n} \log(n) \\ &= \log(n), \end{aligned}$$

because:

$$p(X=i \mid Y=0) = \begin{cases} 1/(n), & \text{if } i \text{ is even} \\ 0, & \text{if } i \text{ is odd} \end{cases}$$

Hence, $H(X \mid Y) = \log(n) = H(X) - 1$.

On the other hand, it is clear that $H(Y \mid X) = 0$, because Y depends on X.

1.16 Let X the variable *belonging to one the neighborhoods* and Y the variable *belonging to a group of answers*. The distribution of Y is $(2p+3)/10$, $(5-2p)/10$ and $1/5$. Hence, the entropy of Y is:

$$H(Y) = -\left(\frac{2p+3}{10}\log\frac{2p+3}{10} + \frac{5-2p}{10}\log\frac{5-2p}{10} + \frac{1}{5}\log\frac{1}{5}\right).$$

On the other hand, the conditioned entropy $H(Y \mid X) = H(3/10, 1/2, 2/10)$. If we compute the maximum of the function:

$$I(p) = H(Y) - H(Y \mid X),$$

we get $I_{\max} = 0.036$ when $p = 1/2$.

1.17 Let's consider the following random variables:

$X =$ "whether it rains or not"

$Y =$ "the meteorologist's prediction"

$Z =$ "the listener's prediction"

with the values 1 whether it rains or there a prediction of rain and 0 otherwise. Looking at the table, we know that the probability that it rains is 1/6 and that it doesn't is 5/6. Hence, the entropy of X is:

$$H(X) = \frac{1}{6}\log 6 + \frac{5}{6}\log\frac{6}{5} = 0.650022.$$

Let's compute now the conditioned entropy $H(X \mid Y)$.

$$\begin{aligned} H(X \mid Y) =& p(X=1,Y=1)\log\frac{1}{p(X=1 \mid Y=1)} \\ &+ p(X=1,Y=0)\log\frac{1}{p(X=1 \mid Y=0)} \\ &+ p(X=0,Y=1)\log\frac{1}{p(X=0 \mid Y=1)} \\ &+ p(X=0,Y=0)\log\frac{1}{p(X=0 \mid Y=0)} \\ =& \frac{1}{12}\log 3 + \frac{1}{12}\log 9 + \frac{1}{6}\log\frac{3}{2} + \frac{2}{3}\log\frac{9}{8} \\ =& 0.607018 \end{aligned}$$

Therefore, the mutual information of X and Y is:

$$I(X,Y) = H(X) - H(X \mid Y) = 0.650022 - 0.607018 = 0.0430047.$$

On the other hand, the joint probabilities of X and Z are given by:

	it rains	it doesn't rains
Predicts it'll rain	0	0
Predicts it wont's rain	1/6	5/6

from we get that both variables are independents. Hence, the mutual information $I(X,Z)$ is zero.

10.2 Codes

2.1 As it is a prefix code, the first three positions are fixed and are 111. The other two can contain any letter. Hence, we can add up to four words.

2.2 Kraft's inequality holds for the first set and so we cannot deduce that $\mathcal{C}$ is a code from the inequality. On the other hand, this set is not a code because the following message can be factorized in two different ways: $00101110 = (001)(01110) = (0010)(1110)$.

The second set $\mathcal{D}$ doesn't fulfill Kraft's inequality and so we deduce it is not a code.

2.4 Let q be the number of symbols. Then by Kraft's inequality we have:

$$\frac{4}{q} + \frac{12}{q^2} \leq 1,$$

from we get that $q \geq 6$.

2.5 By Kraft's inequality, $26/3^\ell \leq 1$. Hence, $\ell \geq \log_3 26$; that is, $\ell \geq 3$.

2.6

1) There is no code with these parameters.

2) $\{1, 000, 001, 010, 0110, 0111\}$.

3) $\{00, 01, 100, 101, 1100, 1101, 11100, 11101\}$.

4) $\{0, 1, 20, 21, 220, 221, 222\}$.

5) There is no code with these parameters.

6) There is no code with these parameters.

2.7 Mimic the proof of Kraft-Macmillan theorem.

For example, the following set is a binary prefix code for which Kraft's inequality is strict:

$$\mathcal{C} = \{00, 010, 011, 1000, 1001, 1010, 1100000, 1100001, \\ 1100010, 1100011, 1100100, 1100101\}.$$

We can add the word 11111111 and the new set is still a prefix code.

10.3 Source Coding

3.2 A possible Huffman code for this source is:

x_1	0	x_2	10	x_3	11	x_4	12
x_5	20	x_6	21	x_7	220	x_8	221.

3.5 A Huffman encoding for S is: $\{0, 10, 110, 111\}$, that has average length 1.9 bits per symbol. Try a Huffman encoding for the second extension S^2.

10.4 Channel Coding

4.4

1) $(p, 1-p)Q = (1/2, p/2, (1-p)/2)$

2) If $p = 1/$, then: $Y = (1/2, 1/8, 3/8)$, $H(Y) = 1.41$, $H(Y|X) = 1$, $I(X, Y) = 0.41$.

3) No.

4.5 If $X = (p_1, p_2, p_3)$ is an input probability distribution, then the output distribution is $Y(q_1, q_2) = (p_1 + p_2, p_3)$. In this situation, the mutual information is given by:

$$I(X,Y) = H(Y) - H(Y \mid X) = H(Y) = -(p_1 + p_2)\log(p_1 + p_2) - p_3 \log p_3,$$

because $H(Y \mid X) = 0$. If we take into account that $\sum p_i = 1$, the channel capacity is the maximum of the function $H(1 - p_3, p_3)$. This maximum is 1 when $p_3 = 1/2$ (considering logarithms to the base 2).

4.6 The input alphabet is $A = \{00, 01, 10, 11\}$ with probabilities p^2, pq, pq and q^2, respectively. On the other hand, the output alphabet is $B = \{0, 1\}$ with probabilities $p^2 + 2pq$ i q^2, respectively. The channel matrix is:

$$Q = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The mutual information of the associated random variables is:

$$I(X,Y) = H(Y) = H(p^2 + 2pq, q^2) = H\left(p^2 + 2p(1-p), (1-p)^2\right).$$

An the maximum value of this function is attained at $p = 1 - \sqrt{2}/2$ and $q = \sqrt{2}/2$ and is equal to 0.693.

10.5 Block Codes

5.1 Supose that x and y differ at positions $i_1, \ldots, i_t$, that is $d(x,y) = t$. At those positions, the word $x \wedge y$ has a zero. If x has a one at position $j \notin \{i_1, \ldots, i_t\}$, then also has y, so that position doesn't make a difference. However that one is counted twice in $|x| + |y|$, and $-2|x \wedge y|$ compensates that. So in the formula $|x| + |y| - 2|x \wedge y|$ we count the number of ones of x and the number of ones of y in the positions $i_1, \ldots, i_t$ and the result is $t = d(x,y)$.

5.2 If $|\mathcal{C}'| < M$, then there are two words $x, y \in \mathcal{C}$ such that $x' = y'$, where x', y' are the words obtained from x, y by erasing the last $d-1$ positions. But this means that x, y differ in at most $d-1$ positions and that's impossible.

5.3 If $x \in \mathcal{C}$, we denote by $\overline{x} \in \overline{\mathcal{C}}$ the word obtained from x by adding a parity bit. If $x, y \in \mathcal{C}$ are at distance d, then $d(\overline{x}, \overline{y}) = d+1$, because d is odd. (Apply the formula of the problem 5.1). Hence the minimum distance of $\overline{\mathcal{C}}$ is less than or equal to $d+1$. Now assume that there are words $\overline{x}, \overline{y} \in \overline{\mathcal{C}}$ at distance d. Then, applying the same formula again, we get that $d(x,y) = d-1$, which is a contradiction. We conclude that the minimum distance of $\overline{\mathcal{C}}$ is $d+1$.

5.4 By problem 5.2, $\mathcal{C}'$ has the same cardinality as $\mathcal{C}$. But $\mathcal{C}'$ has length $n-d+1$, and so $M \leq q^{n-d+1}$.

5.5 The Hamming bound is useless in this case. The Singleton bound yields $A_2(3,2) \leq 9$, and in general $A_p(3,2) \leq p^2$. Now the even parity code of length 3 is an example at which this bound is attained. In general, consider the code:

$$\left\{x_1x_2x_3 \in \mathbb{Z}_p^3 : x_1 + x_2 + x_3 = 0\right\}$$

5.6 Let $x_1, x_2 \in \mathcal{C}_1$ such that $d(x_1, x_2) = d_1$. If $y \in \mathcal{C}_2$, then:

$$d(x_1|x_1 + y, x_2|x_2 + y) = 2d(x_1, x_2) = 2d_1.$$

Analogously, if $y_1, y_2 \in \mathcal{C}_2$ are at distance d_2 and $x \in \mathcal{C}_1$, then:

$$d(x|x + y_1, x|x + y_2) = d(y_1, y_2) = d_2.$$

Hence, $d \leq \min(2d_1, d_2)$.

In general, let $z = x|x+y$, $z' = x'|x'+y'$ be different elements of $\mathcal{C}_1|\mathcal{C}_1+\mathcal{C}_2$. If $y = y'$, then:

$$d(z, z') = 2s(x, x') \geq 2d_1$$

If $y \neq y'$, then:

$$\begin{aligned} d(z, z') &= d(x, x') + d(x + y, x' + y') \\ &= |x + x'| + |(x + y) + (x' + y')| \\ &= d(x + x', 0) + d(x + x', y + y') \\ &\geq d(0, y + y') = d(y, y') \geq d_2 \end{aligned}$$

Thus $d \geq \min(2d_1, d_2)$.

10.6 Finite Fields

6.1 $d(x) = 1$, $a(x) = x^2 + x + 1$, $b(x) = x$.

```
x = PolynomialRing(GF(2), 'x').gen()

d, a, b = xgcd(x^3+1, x^4+x^3+x^2+x+1)
```

6.2 In SAGE we can compute all the powers of an integer a modulo m with the instruction:

```
[a.powermod(k, m) for a in range(1,m)]
```

In this way we can check that 2 is a primitive element of $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_{13}$ but not of $\mathbb{F}_7$. In this latter case we find that 3 is a primitive element. Now, if $a \in \mathbb{F}_p$ is a primitive element, then so is a^k for $\gcd(k, p) = 1$.

Alternatively, we can find the multiplicative orders of all the elements of, for example, $\mathbb{F}_{13}$ with the instructions:

```
R = Integers(13)
[(i, multiplicative_order(i)) for i in R if i != 0]
```

6.3

```
x=PolynomialRing(GF(2),'x').gen();

def irreducible_polynomials_upto_degree (n):
  poly = [x, x+1]
  irred = [x, x+1]
  for i in range(n-1):
    for p in poly:
      if p.degree() == i+1:
        poly.append(p*x)
        poly.append(p*x+1)
        if (p*x+1).is_irreducible():
          irred.append(p*x+1)
  return irred

irred = irreducible_polynomials_upto_degree (6)
primitive = [p for p in irred if p.degree()>1 and p.is_primitive()]
```

Irreducible polynomials:

x
$x+1$
x^2+x+1
x^3+x^2+1
x^3+x+1
x^4+x^3+1
x^4+x+1
$x^4+x^3+x^2+x+1$
x^5+x^3+1
x^5+x^2+1
$x^5+x^4+x^3+x^2+1$
$x^5+x^4+x^3+x+1$
$x^5+x^4+x^2+x+1$
$x^5+x^3+x^2+x+1$
x^6+x+1
$x^6+x^5+x^4+x^2+1$
$x^6+x^5+x^3+x^2+1$
x^6+x^5+1
x^6+x^3+1
$x^6+x^5+x^4+x+1$
$x^6+x^4+x^3+x+1$
$x^6+x^5+x^2+x+1$
$x^6+x^4+x^2+x+1$

Primitive polynomials:

x^2+x+1
x^3+x+1
x^3+x^2+1
x^4+x^3+1
x^4+x+1
x^5+x^3+1
x^5+x^2+1
$x^5+x^4+x^3+x^2+1$
$x^5+x^4+x^3+x+1$
$x^5+x^4+x^2+x+1$
$x^5+x^3+x^2+x+1$
$x^6+x^5+x^3+x^2+1$
x^6+x+1
x^6+x^5+1
$x^6+x^5+x^4+x+1$
$x^6+x^4+x^3+x+1$
$x^6+x^5+x^2+x+1$

6.4

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**4, 'a', modulus=x^4+x^3+x^2+x+1)
a=F.gen()
F.is_field()
  True

[(1+a)^(-1) , (1+a^2+a^3)^(-1)]
  [a^3 + a, a^3 + a^2]

[multiplicative_order(a), multiplicative_order(1+a)]
  [5, 15]

discrete_log((1+a)^(-1), 1+a]
  14

xgcd(1+x, x^4+x^3+x^2+x+1)
  (1, x^3 + x, 1)

xgcd(1+x^2+x^3, x^4+x^3+x^2+x+1)
  (1, x^3 + x^2, x^2 + x + 1)
```

That is: $(1+\alpha)^{-1} = \alpha^3 + \alpha = (1+\alpha)^{14}$ ($1+\alpha$ is a primitive element); $(1+\alpha^2+\alpha^3)^{-1} = \alpha^3 + \alpha^2$.

6.5

```
x=PolynomialRing(GF(2),'x') .gen()
F=GF(2**6, 'a', modulus=x^6+x+1)
a=F.gen()

l= [a^(-1), (1+a^2+a^3)^(-1), (1+a^3+a^4)^(-1)
print l
   [a^5 + 1 , a^5 + a^3 , a^3 + a^2 + a + 1]

multiplicative_order(a)
   63

[a^k for k in divisors(63)]
   [a, a^3, a^2 + a, a^4 + a^3, a^5 + a^4 + a^3 + a + 1, 1]

(x^6+x+1).is_primitive()
   True

[discrete_log(j, a) for j in l]
   [62, 15, 18]
```

Hence, the order of α is 63 and therefore it is a primitive element.

6.6

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**3, 'a', modulus=x^3+x^2+1)
a=F.gen()

(x^3+x^2+1).is_primitive()
   True

multiplicative_order(a)
   7

def zech(j):
   if 1+a^j <> F(0):
      return discrete_log(1+a^j, a)
   else:
      return "error"

[zech(j) for j in range(7)]
   ['error', 5, 3, 2, 6, 1, 4]

((a^2+a^6-a+1)*(a^3+a))/(a^4+a)
   a
```

6.7

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**3, 'a', modulus=x^3+x^2+1)
a = F.gen()

# First method (only works if the matrix is square):
M=matrix(F, [[1,1,1],[1+a,1+a^2,a^3],[1+a,a^2,a]])
e = vector(F, [1,a,a^2])

solutions1 = M.solve_right(e)
   (a + 1, a^2 + a + 1, a^2 + 1)

[discrete_log(j,a) for j in solutions]
   [5, 4, 3]

# The above method doesn't work if the matrix is not square.
# So we solve the system as if the coefficients were symbolic
# expressions in a:
```

```
u,v,w = var('u,v,w')

solve([ (1+a)*u + (1+a^2)*v + a^3*w==0,
        (1+a)*u + a^2*v + a*w==0], u,v,w)
   [[u == (a^4*r1 - a^3*r1 + a^2*r1 - a*r1)/(a + 1),
     v == -a^2*r1 + a*r1 - r1, w == r1]]

# Now we declare r1 as a variable
# and simplify the above solutions in F:

r1=var('r1')

(a^4*r1 - a^3*r1 + a^2*r1 - a*r1)/(a + 1)
  (a^2+a+1)*r1

-a^2*r1 + a*r1 - r1
  (a^2+a+1)*r1
```

Therefore, the solutions to the second system are: $u = v = \lambda\alpha^4$, $w = \lambda$, where $\lambda \in \mathbb{F}_8$.

6.8

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**4, 'a', modulus=x^4+x^3+1)
a=F.gen()

(x^4+x^3+1).is_irreducible()
  True

(x^4+x^3+1).is_primitive()
  True

multiplicative_order(a)
  15

[multiplicative_order(b) for b in a^4,a+a^2,a^5]
  [15, 15, 3]
```

6.9

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**5, 'a', modulus=x^5+x^2+1)
a=F.gen()

discrete_log( a^5+a^23+(a^2+a^4)/(1+a^12), a)
  22
```

```
solutions = [b for b in F if a^3*b^2+a^18*b+1==0]
print solutions
  [a^3 + a, a^4 + a^2 + 1]

[discrete_log(c, a) for c in solutions]
  [6, 22]
```

Another method for computing the roots of a polynomial consists of applying the method `.roots()` to a polynomial with coefficients in the finite field. This method returns a list of pairs consisting of a root and its multiplicity. First we must define the polynomial ring with coefficients in $\mathbb{F}_{32}$:

```
t = PolynomialRing(F, 't').gen()
rts=(a^3*t^2+a^18*t+1).roots()
  [(a^3 + a, 1), (a^4 + a^2 + 1, 1)]

[discrete_log(b, a) for (b,_) in rts]
  [6, 22]
```

6.10

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**4, 'a', modulus=x^4+x+1)
a=F.gen()

solutions = [t for t in F if a^3*t^3+a^2*t^2+a^6*t+1==0]
print solutions
  [a + 1, a^2 + a + 1, a^3 + a^2 + 1]

[discrete_log(t, a) for t in solutions]
  [4, 10, 13]

# Another way:
t = PolynomialRing(F, 't').gen()
rts = (a^3*t+a^2*t^2+a^6*t+1).roots()
rts = [b for (b,_) in rts]
```

6.11

```
x=PolynomialRing(GF(2),'x').gen()
F=GF(2**4, 'a', modulus=x^4+x+1)
a=F.gen()

def p(t):
  return t^13+t^12+t^6+t^5+t^4+t^2+t+1
```

```
[p(a^i) for i in range(1,7)]
  [a^3 + a^2, a^3 + a^2 + a + 1, a^2 + 1, a^3 + a, a^2 + a + 1, a]

result = map(p, [a^i for i in range(1,7)])
print result
  [a^3 + a^2, a^3 + a^2 + a + 1, a^2 + 1, a^3 + a, a^2 + a + 1, a]

[discrete_log(b, a) for b in result]
  [6, 12, 8, 9, 10, 1]
```

6.12

```
x=PolynomialRing(GF(2), 'a').gen()
F=GF(2**16, 'a', modulus=x^4+x+1)
a=F.gen()
t=PolynomialRing(F, 't').gen()

p1=t^4
p2=a^11*t^3+a^5*t^2+a^13*t+a^14

xgcd(p1, p2)
  (1, (a^3 + a^2 + a + 1)*t + a, a*t^2 + t + a)
```

10.7 Linear Codes

7.2 A systematic generator matrix is:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and so a systematic encoding for $\mathcal{C}$ is $a_1a_2a_3 \mapsto (a_1, a_2, a_3, a_1, a_1 + a_2 + a_3)$. Thus:

$$\mathcal{C} = \{00000, 00101, 01001, 01100, 10011, 10110, 11010, 11111\}$$

We observe that the minimum weight of a nonzero codeword is 2. Hence, $d = 2$. A parity-check matrix can be written from G_1 as:

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

It is also possible to read d from H_1: there are two linearly dependent columns (e.g., the second and the third), but any set of one column is linearly independent (that is, nonzero).

7.7 Let $\mathcal{C}$ be a linear code with parameters $[n,k,d]_2$. Let H be a parity matrix of $\mathcal{C}$. We know that the rank of H is $n-k$. Now we have that all codewords have a even number of ones if, and only if, they satisfy the equation $x_1+\cdots+x_n=0$. Assume that $\mathcal{C}$ has word with odd number of ones. Then the matrix:

$$\begin{bmatrix} & H & \\ 1 & \cdots & 1 \end{bmatrix}$$

has rank $n-k+1$, because the last equation is independent from the rest. Hence it is the parity check matrix of a new code (in fact, a sobcode of $\mathcal{C}$) of dimension $n-(n-k+1)=k-1$. Thus the number of codewords of $\mathcal{C}$ with an even number of ones is $2^{k-1}=2^k/2=|\mathcal{C}|/2$.

7.8 Parameters: length $n=sr$, dimension $k=s+r-1$, minimum distance $d=4$. Hence we can use this code to detect 1 error and correct 2 errors, simultaneously.

7.9 Let x be the word received and let s be the number of zeros of x.

1) If $0\leq s\leq 2$, then we decode x as $1\cdots 1$.

2) If $5\leq s\leq 7$, then we decode x as $0\cdots 0$.

3) If $3\leq s\leq 4$, then we announce that 3 or 4 errors have ocurred.

7.11 Computing the syndrome corresponding to a given leader is a linear operation, so if $(y_1,\cdots,y_6)$ is the leader corresponding to (s_1,s_2), then we can take $\lambda\cdot(y_1,\ldots,y_6)$ as the leader corresponding to $\lambda\cdot(s_1,s_2)$. Hence we can list only the leaders corresponding to the syndromes 00, 01, 10, 11, 1α and $1\alpha^2$.

s	00	01	10	11	1α	$1\alpha^2$
ℓ	00000	00001	00010	10000	01000	00100

7.12 Parameters: $n=5,k=2,d=2$. Hence $|\mathcal{C}|=2^2=4$. The syndrome of a word $y=y_1y_2y_3y_4y_5$ is given by $s(y)=(y_2+y_5,y_3+y_5,y_1+y_4+y_5)$. The table of syndromes, cosets and possible leaders is the following:

s	coset			
000	00000	10010	11101	01111
001	10000	<u>00010</u>	01101	11111
010	00100	10110	11001	01011
011	10100	<u>00110</u>	<u>01001</u>	11011
100	01000	11010	10101	00111
101	11000	<u>01010</u>	<u>00101</u>	00111
110	01100	01110	<u>10001</u>	<u>00011</u>
111	00001	10011	11100	01110

A possible leader is written in the first position of each coset; whenever there is more than one possible leader, the other ones are underlined. The words in the first coset are the codewords.

The syndrome of $y = 01001$ is $s(y) = 011$. Hence, using the above table, the corresponding leader is 10100. So we decode y as $y - 10100 = 11101$.

7.15 The length is $n = (q^r - 1)/(q - 1) = (3^r - 1)/(3 - 1) = 4$. Thus $r = 2$. The matrix is given by:

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix}$$

7.18 The matrix is:

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \alpha & \alpha^2 \end{bmatrix}$$

The syndrome of $0\alpha\alpha11$ is $0\alpha^2$; that is, it's α^2 times the first column of H. Hence there is an error in the first position of magnitude α^2. The corrected word is then $0\alpha\alpha11 + \alpha^2 0000 = \alpha^2 0\alpha\alpha11$.

10.8 Cyclic Codes

8.1

1) $x^3 + 1 = (x + 1)(x^2 + x + 1)$

2) $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$

3) $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. We get this factorization as follows. First we compute the cyclotomic classes of 2 mod 7:

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4\}, \quad C_3 = \{3, 5, 6\}$$

This means that $x^7 + 1$ factors as:

$$\begin{aligned} x^7 + 1 &= f_{C_0}(x) \cdot f_{C_1}(x) \cdot f_{C_3}(x) \\ &= (x + 1) \cdot [(x + \alpha)(x + \alpha^2)(x + \alpha^4)] \cdot [(x + \alpha^3)(x + \alpha^5)(x + \alpha^6)] \\ &= (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \end{aligned}$$

where α is the class of x in $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$ and the computations are done in this field.

4) $x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$. First we compute the cyclotomic classes mod 9:

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8, 7, 5\}, \quad C_3 = \{3, 6\}$$

So x^9+1 has three irreducible factors of degrees 1, 6 and 2, respectively. Now the order of 2 mod 9 is 6, so we have to work in $\mathbb{F}_{2^6}=\mathbb{F}_{64}=\mathbb{F}_2[x]/(x^6+x+1)$. (Check that x^6+x+1 is a binary primitive polynomial.) Then the factorization of x^9+1 is:

$$\begin{aligned} x^9+1 &= f_{C_0}(x)\cdot f_{C_1}(x)\cdot f_{C_3}(x) \\ &= (x+1)\cdot\prod_{j\in C_1}(x+\omega^j)\cdot\prod_{j\in C_3}(x+\omega^j) \\ &= (x+1)(x^6+x^3+1)(x^2+x+1) \end{aligned}$$

where $\omega=\alpha^{(2^6-1)/9}=\alpha^7$.

8.2 The generator polynomial $g(x)$ is a divisor of x^5-1, and this polynomial factors as $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$. Therefore, there are $2^2=4$ cyclic codes of length 5.

- $g(x)=1$: the total code $\mathbb{F}_2^5$.
- $g(x)=x-1$: the even code, the code consisting of those words with even weight.
- $g(x)=x^4+x^3+x^2+x+1$: the repetition code.
- $g(x)=x^5-1$: the trivial code with only one word 00000.

Let $\mathcal{C}$ be the cyclic code of length 7 with generator polynomial $g(x)=1+x^2+x^3$. Then the parity-check polynomial is $h(x)=(x^7-1)/g(x)=1+x+x^2+x^3+x^4$. From this polynomial we can write the parity-check matrix:

$$H=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

As we see, the columns of H are all non-zero binary words of length 3, so H is equivalent to the standard binary Hamming code of codimension 3.

8.4 Assume that $\mathcal{C}$ has codeword a of odd weight. Then $a(1)\neq 0$, so $g(1)\neq 1$, where $g(x)$ is the generator polynomial of $\mathcal{C}$. This implies that $g(x)$ is a divisor of $(x^n-1)/(x-1)=x^{n-1}+\cdots+x+1$, so this last polynomial is codeword. Hence $11\cdots 1\in\mathcal{C}$.

Reciprocally, if $11\cdots 1\in\mathcal{C}$ and the length of $\mathcal{C}$ is odd, then $\mathcal{C}$ has a codeword of odd weight.

8.5 It's easy to check that $g(x)=1+x+x^2+x^3 \mid (x^8-1)$. The dimension is $n-\deg(g)=8-3=5$. To encode systematically $M(x)=1+x^2+x^4$, we multiply it by $x^{\deg(g)}=x^3$ and divide the result by $g(x)$:

$$x^3M(x)=g(x)(x^4+x^3+x^2+x)+x$$

Hence, we encode M as $x+x^3M(x)$, that is as 010 10101.

8.6 If $M(x) = 1 + x + x^3$, then $x^3M(x) = g(x)(x^3 + x^2) + x^2$. Hence we encode M as 001 1101.

8.7 First we observe that dimension is $6 - 4 = 2$. So the cardinality of this code is $2^2 = 4$. The codewords are of the form $p(x)g(x)$, where $p(x)$ is a binary polynomial of degree at most 1. Hence the code is:

$$\{0, g(x), xg(x), (1 + x)g(x)\}$$

The minimum distance is 4.

8.8 The first exponent $n \geq 5$ such that $g(x) = x^4 + x^3 + x^2 + 1$ divides $x^n - 1$ is $n = 7$. If we take $n = 7$, then the dimension is $k = 3$, the cardinality of the code is $2^k = 2^3 = 8$, the parity-check polynomial is $h(x) = (x^7 - 1)/g(x) = 1 + x^2 + x^3$ and a parity-check matrix is given by:

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

The matrix H has 4 linearly dependent columns (the sum of the columns 1, 2, 3, and 6 is zero), so $d \leq 4$. Moreover, any set of 3 columns is linearly independent, because the rank H is 4. Hence $d = 4$. We encode the information string $p_0p_1p_2$, corresponding to the coefficients of $p(x) = p_0 + p_1x + p_2x^2$, as:

$$p_0p_1p_2 \mapsto r_0r_1r_2r_3p_0p_1p_2$$

where $r_0 = p_0 + p_1$, $r_1 = p_1 + p_2$, $r_2 = p_0 + p_1 + p_2$, $r_3 = p_0 + p_2$. For example, the string 001 is encoded as 0111 001. The list of Meggitt's algorithm contains all polynomials of degree less or equal than 6 and weight at most 1 and their corresponding syndromes.

leader	x^6
syndrome	$x^3 + x^2 + x$

For example, let's apply this algorithm to correct the errors in the word $y = 0110001 \leftrightarrow x + x^2 + x^6$. The syndrome is $s(y) = x^3$. The algorithm yields:

i	6	5	4	3
s	x^3	$x^3 + x^2 + 1$	$x^2 + x + 1$	$x^3 + x^2 + x$

Hence y has an error at the position 3.

8.10 The dimension is $k = 15 - 4 = 11$. The polynomial corresponding to this message is $M(x) = 1 + x + x^4 + x^5 + x^7 + x^9 + x^{10}$ and $x^4M(x)$ is a multiple of $g(x) = 1 + x + x^4$ (in fact, $M(x) = (1 + x + x^4) + x^5(1 + x + x^4) + x^6(1 + x + x^4) = (1 + x + x^4)(1 + x^5 + x^6)$). Hence the message is encoded as: 0000 11001101011.

The minimum distance is 3 (prove this!), so $\rho = 1$. The table L consists of x^{14} and its syndrome $s(x^{14}) = x^3 + 1$. Let $y(x) = x^4 + x^8 + x^9 + x^{11} + x^{13} + x^{14}$ the polynomial

corresponding to the word received. Its syndrome is $s(y) = x^2 + x$. Meggitt's algorithm gives:

i	14	13	12	11	10
s	x^2+x	x^3+x^2	x^3+x+1	x^2+1	x^3+x
i	9	8	7	6	5
s	x^2+x+1	x^3+x^2+x	x^3+x^2+x+1	x^3+x^2+1	x^5+1

Therefore, there is an error in the 5th position.

8.12

1) The word 011 corresponds to the polynomial $x+x^2$. If we multiply it by x^6 and divide the result by $g(x)$, we get:

$$x^8 + x^7 = g(x)(x^2 + x) + (x^5 + x^4 + x^2 + x)$$

Hence, we encode 011 as 011011011.

2) First, we construct the table of leaders and syndromes. As $d = 3$, this code can correct at most one error. Hence we assume this error is at the last position and so this table has only one entry: that corresponding to the polynomial x^8 with syndrome $x^5 + x^2$. Now the syndrome of the received word $y(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^7 + x^8$ is $s(y) = x^4 + x$. As this syndrome is not in the list, we shift the word to the right and now the position to be corrected is the seventh. The new word's syndrome is gotten by multiplying the old one by x. So the new syndrome is $x^5 + x^2$, that is in the list. So we conclude that the received word has an error at the seventh position and the corrected word is: 101101101.

8.13

1) As $g(1) = 0$, all multiples of $g(x)$ also vanish at 1. Hence all codewords have an even number of ones (even weight).

2) The dimension is 3, so we split the message into two parts and encode each part separately. The word 001 is represented as the polynomial x^2. If we multiply it by x^4 and divide the result by $g(x)$, we get:

$$x^6 = g(x)q(x) + (x^3 + x^2 + x)$$

Hence, we encode 001 as 0111 001. Analogously, the second word 101 is encoded as 1100 101.

3) First, we construct the table of leaders and syndromes. As $d = 3$, this code can correct at most one error. Hence we assume this error is at the last position and so this table L has only one entry: that corresponding to the polynomial x^6 with syndrome $x^3 + x^2 + x$.

Now the syndrome of the received word $y(x) = x+x^3+x^4+x^5+x^6$ is $s(y) = x^3+x^2+x$. As $s(y) \in L$, we announce that y has an error in the last position. We correct it as 0101110.

For the second word $z(x) = 1 + x^3 + x^4 + x^5 + x^6$, we have: $s(z) = x^3 + x^2 + 1$. this syndrome does not belong to L. We apply the algorithm: we cyclically shift z one position to the right. The new syndrome is $s(xs(z)) = x^2 + x + 1 \notin L$. We cyclically shift another position to the right and get the syndrome $x^3 + x^2 + x \in L$. That is, there is an error in the 4th position and we correct z as 1001011.

8.14

1) $y = 1 + x + x^5 + x^6 + x^{10} + x^{11} + x^{12} + x^{13}$; $s = (\alpha, \alpha^{12})$; y has more than 2 errors.

2) $y = x^6 + x^7 + x^8 + x^{10} + x^{14}$; $s = (\alpha^6, 0)$; y has 2 errors at the positions 1 and 11.

3) $y = 1 + x + x^3 + x^4 + x^6 + x^7 + x^{11} + x^{12}$; $s = (\alpha^{11}, \alpha^6)$; y has more than 2 errors.

4) $y = 1 + x + x^2 + x^4 + x^5 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14}$; $s = (\alpha^9, \alpha^2)$; y has 2 errors at the positions 2 and 11.

5) $y = x^2 + x^7 + x^8 + x^{10} + x^{14}$; $s = (\alpha^2, \alpha^2)$; y has more than 2 errors.

6) $y = x + x^4 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{14}$; $s = (\alpha^{10}, \alpha^3)$; y has more than 2 errors.

10.9 BCH and Reed-Solomon Codes

9.3 The cyclotomic classes (of 2 modulo 15) we are interested in are C_3, C_4 and C_5. But:

$$C_3 = \{3, 6, 12, 9\}, \quad C_4 = \{4, 8, 1, 2\}, \quad C_5 = \{5, 10\}.$$

Hence the degree of the generating polynomial $g(x)$ is $|C_3| + |C_4| + |C_5| = 10$ and the dimension of the code is $15-10 = 5$. The polynomial $g(x)$ vanishes at $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$, so the designed distance is $\delta = 7$. Hence, $d \geq \delta = 7$ and $\mathcal{B}$ can correct at least 3 errors.

9.4 The generating polynomial $g(x)$ vanishes at α^i, for $i = 1, 2, 3, 4, 5, 6$. Hence, we need the following cyclotomic classes mod 31: $C_1 = \{1, 2, 4, 8, 16\}$, $C_3 = \{3, 6, 12, 24, 17\}$ and $C_5 = \{1, 5, 10, 20, 9, 18\}$. Thus,

$$\begin{aligned} g(x) &= m_1(x)m_3(x)m_5(x) \\ &= (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1) \\ &= x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1. \end{aligned}$$

The length is $n = 31$; the dimension: $k = n - \deg(g) = 31 - 15 = 16$ (16 information bits and 15 redundancy bits). A lower bound for the minimum distance: $d \geq \delta = 7$. Hence this code can correct up to 3 errors.

We have:

$$y(\alpha) = \alpha^2, \quad y(a^3) = \alpha^{20}, \quad y(\alpha^5) = \alpha^9.$$

Then the syndrome polynomial of y is:

$$s(x) = \alpha^9 x^5 + \alpha^{13} x^4 + \alpha^8 x^3 + \alpha^{20} x^2 + \alpha^4 x + \alpha^2.$$

We have:

$$\begin{aligned} b_1(x) &= q_1(x) = \alpha^{22} x + \alpha^{26} \\ b_2(x) &= 1 + b_1(x) q_2(x) = \alpha^{16} x^2 + \alpha^{24} x + \alpha^{29} \\ b_3(x) &= b_1(x) + b_2(x) q_3(x) = \alpha^{22} x^3 + \alpha^{10} x^2 + \alpha^{30} x + \alpha^{28}. \end{aligned}$$

So $\ell(x) = b_3(x)/b_3(0) = \alpha^{25} x^3 + \alpha^{13} x^2 + \alpha^2 x + 1$. Finally, the roots of $\ell(x)$ are 1, α and α^5, so the error locators (their inverses) are: 1, α^{30} and α^{26}, and the word sent is:

$$\underline{1}0001111000010000110101111\underline{1}0001\underline{}$$

9.5

1) The generating polynomial $g(x)$ vanishes at $\alpha, \alpha^2, \alpha^3, \alpha^4$. Hence:

$$\begin{aligned} g(x) &= m_\alpha(x) m_{\alpha^3}(x) \\ &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

2) The dimension is $15 - 8 = 7$ and $d \geq \delta = 5$. Hence this code can correct at least 2 errors.

3) $M(x) = x + x^2 + x^3 + x^5$. We multiply $M(x)$ by x^8 and divide by $g(x)$:

$$M(x)x^8 = g(x)q(x) + (x^7 + x^6 + x^5 + x^4 + x^3 + x^2)$$

Hence we encode M as $x^{13} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2$ or as the corresponding binary string 001111110111010.

4) Let $y(x) = 1 + x + x^4 + x^5 + x^6 + x^{11} + x^{12} + x^{13} + x^{14}$. We have: $s_1 = y(\alpha) = \alpha^{12}$ and $s_2 = y(\alpha^3) = \alpha^{11}$. Now $s_1^3 = (\alpha^{12})^3 = \alpha^6 \neq \alpha^{11}$. Therefore the word contains more than one error. Now we try to solve the quadratic equation $T^2 + s_1 T + (s_1^3 + s_2)/s_1 = T^2 + \alpha^{12} T + \alpha^4 = 0$. This equation has two solutions: α^5 and α^{14}. So we announce that y has two errors at positions 5 and 14 and correct it as 11001 01000 01110.

5) We already know that $y(\alpha) = \alpha^{12}$ nd $y(\alpha^3) = \alpha^{11}$, so we can write the syndrome polynomial:

$$\begin{aligned} s(x) &= y(\alpha) + y(\alpha^2)x + y(\alpha^3)x^2 + y(\alpha^4)x^3 \\ &= \alpha^{12} + \alpha^9 x + \alpha^{11} x^2 + \alpha^3 x^2 \end{aligned}$$

as $y(\alpha^2) = y(\alpha)^2 = (\alpha^{12})^2 = \alpha^9$ and $y(\alpha^4) = y(\alpha^2)^2 = (\alpha^9)^2 = \alpha^3$.

Now we apply the extended Euclid algorithm to $x^{\delta-1} = x^4$ and $s(x)$ until we get a remainder with degree less than $\lfloor(\delta-1)/2\rfloor = 2$. Then we compute the polynomials $b_1(x), b_2(x)$:

$$b_{-1} = 0, b_0 = 1, b_1 = q_1, b_2 = 1 + q_1 q_2$$

That is $\ell(x) = b_2(x) = 1 + (\alpha^{12}x + \alpha^5)\alpha^7 x = \alpha^4 x^2 + \alpha^{12}x + 1$. The roots of this polynomial are α and α^{10}. Their inverses give us the error positions: 14 and 5, respectively.

9.6 Thanks to Franziska Bertelshofer (2011) for her solution using SAGE.

1) First we construct the ring of binary polynomials and check that the given polynomial is primitive.

```
x = PolynomialRing(GF(2), 'x').gen()
(x^6 + x^4 + x^3 + x + 1).is_primitive()

  True
```

Now we can build $\mathbb{F}_{16}$ out from that polynomial.

```
F = GF(2^6, 'a', modulus = x^6+x^4+x^3+x+1)
a = F.gen()
```

2) We define some generic functions that will be useful later on.

```
# Cyclotomic class of j mod n:
def cyclo(j, n):
        c = [j]
        r = 2 * j
        q = mod(2 * j, n)
        while q != j:
                c = c + [q]
                r = 2 * r
                q = mod(r, n)
        return tuple(sorted(c))

# All cyclotomic classes up to delta-1:
def all_cyclo(n, delta):
        return [(i,cyclo(i,n)) for i in xrange(1,delta-1) \
                if mod(i, 2) !=0]
```

The designed distance of this code is $\delta = 10$, so we only need to construct the cyclotomic classes C_i, for $i = 1, \ldots, 9$.

```
cyclos = all_cyclo(63, 11)
for (i,j) in cyclos:
        print "C_" + str(i) + " = " + str(j)
```

And we get:

$$C_1 = \{1, 2, 4, 8, 16, 32\}$$
$$C_3 = \{3, 6, 12, 24, 33, 48\}$$
$$C_5 = \{5, 10, 17, 20, 34, 40\}$$
$$C_7 = \{7, 14, 28, 35, 49, 56\}$$
$$C_9 = \{9, 18, 36\}$$

3) Now we compute the generator polynomial from these cyclotomic classes:

$$g(t) = \prod_C \prod_{i \in C} (t - \alpha^j)$$

where C varies among the set of cyclotomic classes. We perform the operations in the polynomial ring $\mathbb{F}_{64}[t]$.

```
t = PolynomialRing(F, 't').gen()
g = prod([prod((t-a^i) for i in j) for (_,j) in cyclos])
print "g(t) = ", g
```

And the result is:

$$g(t) = t^{27} + t^{26} + t^{25} + t^{24} + t^{23} + t^{20} + t^{19} + t^{15} + t^{11} + t^9 + t^8 + t^7 + t^6 + t^5 + t^3 + t + 1$$

4) The parameters of $\mathcal{B}$ are: length $n = 63$, dimension $k = n - \deg(g) = 63 - 27 = 36$, lower bound for the minimum distance $d \geq \delta = 10$, and a lower bound for the number of errors the code can correct $\rho \geq 4$. Since the cyclotomic class C_{10} is equal to C_5, we get the same code when the designed distance is 11. So we can improve this value and put $\delta = 11$ and then we get $d \geq 11$ and $\rho \geq 5$. That is, our code can correct at least 5 errors.

5) We define a couple of functions, one to convert a bit string to a polynomial and another one to encode systematically a bit string.

```
def string_to_polynomial (M, t):
        return sum(M[i] * t^i for i in range(len(M)))

def encode(M, g, t):
        m = string_to_polynomial(M, t)
        d = t^(g.degree()) * m
        r = d.mod(g)
        c = d - r
        return (c, c.coeffs())
```

Now we can encode the string given in the problem.

```
M = [1]*12 + [0]*12 + [1]*12
(n, N)= encode(M, g, t)
print "N = ", N
```

```
  N =  [1, 1, 1, 0, 1, 0, 1, 0, 0 ,0 ,0 ,0 ,0, 1, 0, 0,
  1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
```

6) Now we introduce two errors at position 18 and 40 (where we start counting at 0).

```
Np = N
Np[18] = 1 - Np[18]
Np[40] = 1 - Np[40]
np = string_to_polynomial(Np, t)
```

We compute the syndrome of this word as a pair of elements of $\mathbb{F}_{64}$.

```
# Compute the syndrome:
s1 = np(a)
s2 = np(a^3)
print "s = (s1, s2) =", s1, "," , s2
print "s1^3 == s2?: ", s1^3 == s2
```

```
  s = (s1, s2) = a, a^4
  s1^3 == s2?: False
```

```
# 2 errors at least. Solve a quadratic equation:
err = t^2 + s1*t + (s1^3+s2)/s1
print "solutions: ", err.roots()
print "error positions: ", [root.log(a) for (root,_) in err.roots()]
```

```
  solutions: [(a^4 + a^2 + 1, 1), (a^4 + a^2 + a + 1, 1)]
  error positions: [40, 18]
```

7) Recall that the syndrome polynomial associated with the word p is:

$$s(t) = \sum_{i=0}^{\delta-2} s_i t^i, \quad s_i = p(\alpha^{i+1})$$

Once we have $s(t)$, we apply the euclidean algorithm to $t^{\delta-1}$ and $s(t)$.

```
# Calculate the syndrome polynomial:
def syndrome(n, a, d):
        return sum([n(a^(i+1))*t^i for i in range(d-1)])
```

```
# Adapted Euclidean algorithm
def euclid(s, d, t):
        (q, r) = (t^(d-1)).quo_rem(s)
        (ra, rb) = (s, r)
        b = [1,q]
        while r.degree() >= (d-1)/2
                (q, r) = ra.quo_rem(rb)
                b = b + [b[-2] - b[-1]*q]
                (ra, rb) = (rb, r)
        return b[-1]

P = [0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
     1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1,
     0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1,
     1, 0, 0]
p = string_to_polynomial(P, t)

# We try to correct p assuming that delta = 10:
s = syndrome (p, a, 10)
b = euclid(s, 10, t)
# Error locator polynomial:
(l, _) = b.quo_rem(b(0))
l.roots()
errors = [63 - root.log(a) for (root,_) in l.roots()]

# Check wether the corrected word is a codeword:
p_corrected = (p - sum([t^i for i in errors]))
p_corrected.mod(g) == 0
  False

# Try again with delta = 11    :
s = syndrome (p, a, 11)
b = euclid (s, 11, t)
(l, _) = b.quo_rem(b(0))
l.roots()
errors = [63 - root.log(a) for (root,_) in l.roots()]
  [60, 50, 45, 20, 55]

# Check wether the corrected word is a codeword:
p_corrected = (p - sum([t^i for i in errors]))
p_corrected.mod(g) == 0
  True

# Finally the correct binary word (corresponding to the
# coefficients of p) is:
str(p_corrected.coeffs)+ [0, 0, 0]
```